

CLAIMS

Sub A

1. A method for cryptographic conversion of binary data blocks comprising splitting said data blocks into $N \geq 2$ subblocks, alternate converting said blocks by performing on the i -th subblock, where $i \leq N$, at least one conversion operation dependent on the value of j -th subblock, characterised in that an operation of transposing bits of i -th subblock is used as the operation dependent on the value of j -th subblock, where $j \leq N$.

2. A method according to claim 1, characterised in that said operation of transposing bits of said i -th subblock which depends on the value of j -th subblock is generated depending on a secret key before the beginning of i -th subblock conversion.

3. A method according to claim 1, characterised in that before performing the current operation of transposing bits of said i -th subblock, which depends on the value of said j -th subblock, a binary vector V is additionally generated, said operation of transposing bits of said i -th subblock being performed depending on the V value, whereby said binary vector is generated depending on its value at the time of performing the preceding step of converting one of said subblocks and depending on the j -th subblock value.

00582206 "071700